UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/507,190	09/09/2004	Pim Theo Tuyls	NL 020192	1803

24737 7590 08/04/2008
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
TRAORE, FATOUMATA	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
08/04/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Advisory Action Before the Filing of an Appeal Brief	Application No.	Applicant(s)	
	10/507,190	TUYLS ET AL.	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2136	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 10 July 2008 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____months from the mailing date of the final rejection.
   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.
   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.
   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: *5-8*.
   Claim(s) rejected: *1-4 and 9-20*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
13. ☐ Other: _____.

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136

Continuation of 11. does NOT place the application in condition for allowance because: With regard to the prior art rejection, Applicant argues that "[n]either Leighton nor Hoffstein teaches or suggests calculating a common secret between two parties as a product of two symmetrical polynomials." According to Applicant, "the Office action fails to identify which of Hoffstein's terms are asserted to be a secret that is common to the parties", "the above text fails to identify any of Hoffstein's terms as being a symmetrical polynomials, and specifically does not identify any of the calculated terms as being a product of two symmetrical polynomials." See response at page 9 of 11.
The examiner respectfully disagrees.
Applicant acknowledges that steps 1-4 of Hoffstein's Figure 5 teach the calculation of a polynomial h(x) as the product of two polynomials, g(x) and (f(x) + c(x)). However, Applicant contends that "the applicants respectfully note that nowhere in Hoffstein are the polynomials g(x) and (f(x) + c(x)) taught to be symmetrical polynomials.
It should be noted that a symmetrical polynomial (or algorithm) uses a secret or private key (or value), while an asymmetrical polynomial (or algorithm) uses two keys or values (a public key and a private key). The examiner submits that the polynomials of Hoffstein are symmetrical polynomials.
Hoffstein discloses that the polynomials are private key polynomials. Hoffstein discloses a first polynomial and a second polynomial, wherein the constraints on the polynomials are selected such that an attacker will find it very difficult to recover the private key polynomial from the partial information sent between the prover (first party) and verifier (second party). See abstract.
Leighton and Hoffstein disclose a first party holding a symmetrical polynomial P(x,y) fixed in the first argument by a value p1 and a symmetrical polynomial Q(x,y) fixed in the first argument by a value q1, and sends the values p1 and q1 to a second party. See, for example, Leighton at column 4, lines,55-65 and Hoffstein in figures 1A and 1B.
Furthermore, Leighton et al discloses that a pair of users or parties I and j use their individual keys to compute a common secret key. See abstract; column 4, lines 55-65.
It is submitted that the combination of Hoffsteing and Leighton discloses the claimed limitations. Accordingly, the rejection is maintained..